[19]中华人民共和国专利局

[11] 公开号 CN 1131992A

# [12] 发明专利申请公开说明书

[21]申请号 95190768.9

[51]Int.Cl[6]
G06F 9/06

[43]公开日 1996 年 9 月 25 日

[22]申请日 95.7.5

[30]优先权

[32]94.7.5 [33]JP[31]174933/94

[86]国际申请 PCT/JP95/01344 95.7.5

[87]国际公布 WO96/01450 日 96.1.18

[85]进入国家阶段日期 96.4.15

[71]申请人 株式会社前进

地址 日本东京都

[72]发明人 渡边晋一郎

久林靖孝

[74]专利代理机构 中国专利代理(香港)有限公司

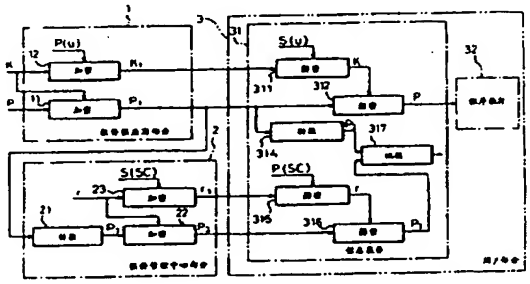
代理人 王 勇 邹光新

权利要求书 3 页 说明书 10 页 附图页数 2 页

[54]发明名称 软件保护系统

[57]摘要

本发明提出了一种软件保护系统。在该系统中，只有经过授权的用户才可以对软件进行操作，其他用户则不能使用该软件，并且能够检测到对该软件的非法改动同时发出警报。该系统主要有以下三个部分组成：软件供应商部分，随时准备为软件管理中心部分和用户部分提供程序；软件管理中心部分；转换提供的程序并随时准备将此经过转换的程序提供给用户部分；用户部分，转换提供的程序，并将此经过转换的程序与上述由软件管理中心所提供的经过转换的程序相比较，只有二者相同时才去执行该程序。



# 权利要求书

1. 一个保护软件的系统，包括：软件供应商部分，随时准备为软件管理中心部分和用户部分提供程序；软件管理中心部分，与上述软件供应商部分相连，按预定的方式转换所提供的程序并随时准备将此经过转换的程序提供给用户部分；用户部分，与上述软件供应商部分和软件管理中心部分相连，按预定的方式转换所提供的程序，并将此经过转换的程序与上述由软件管理中心所提供的经过转换的程序相比较，只有二者相同时才去执行该程序。

2. 根据权利要求1的系统，其中，程序要加密；并且，当用户部分判定程序可执行时，要对经过加密的程序进行解密。

3. 根据权利要求1的系统，其中，由软件管理中心部分向用户部分提供的经过转换的程序要加密，并且，至少当用户部分使用该程序时，要对经过加密的程序进行解密。

4. 根据权利要求2的系统，其中，在软件供应商部分，使用基于公共文件或来自用户的请求的密钥对程序进行加密，并且，在用户部分，使用保密密钥对经过加密的程序进行解密。

5. 根据权利要求3的系统，其中，在软件管理中心部分，使用软件管理中心部分的保密密钥对经过转换的程序进行加密，并且，在用户部分，使用软件管理中心部分的公开密钥对经过加密的程序进行解密。

6. 根据权利要求2的系统，其中，在软件供应商部分，使用用户部分公用的密钥对程序进行加密，该密钥是在特定于软件或软件供应商部分的保密算法中应用用户部分的标识符所生成的，并且，在用户部

分，使用软件或软件供应商部分公用的密钥对经过加密的程序进行解密，该密钥是在特定于用户部分的保密算法中应用软件或软件供应商部分的标识符所生成的。

7. 依据权利要求3的系统，其中，在软件管理中心部分，使用用户部分和软件或软件供应商部分公用的密钥对经过转换的程序进行加密，该密钥是在特定于软件或软件供应商部分的保密算法中应用用户部分的标识符所生成的，并且，在用户部分，使用软件或软件供应商部分公用的密钥对经过加密和转换的程序进行解密，该密钥是在特定于用户部分的保密算法中应用软件供应商部分的标识符所生成的。

8. 一个保护软件的系统，包括：软件供应商部分，使用第一密钥对程序进行加密得到一经过加密的程序，再使用第二密钥对第一密钥进行加密得到经过加密的第一密钥，然后将此经过加密的程序提供给软件管理中心部分，并随时准备将此经过加密的程序和经过加密的第一密钥提供给用户部分；软件管理中心部分，与上述软件供应商部分相连，对提供的经过加密的程序进行转换得到一经过转换和加密的程序，然后使用第三密钥对该经过转换的程序进行加密得到一经过加密和转换的程序，再使用第四密钥对第三密钥进行加密得到经过加密的第三密钥，并随时准备将此经过加密和转换的程序及经过加密的第三密钥提供给用户部分；用户部分，与上述软件供应商部分和软件管理中心部分相连，在使用程序期间，按预定的方式对经过加密的程序进行转换得到经过转换的程序，然后使用第五密钥对经过加密的第三密钥进行解密得到解了密的第三密钥，再使用第三密钥对经过加密和转换的程序进行解密得到解了密的经过转换的程序，将此解了密的经过转换的程序与上述经过转换的程序相比较，只有当二者相同时才使用

第六密钥解密第一密钥，然后使用该第一密钥去解密并执行该程序。

9. 根据权利要求8的系统，其中，第二密钥是用户部分的公开密钥，第六密钥是用户部分的保密密钥，第四密钥是软件管理中心部分的保密密钥，第五密钥是软件管理中心部分的公开密钥。

10. 根据权利要求8的系统，其中，第二密钥是用户部分公用的密钥，该密钥是在软件或软件供应商部分的保密算法中应用用户部分的标识符所生成的，第五和第六密钥是软件或软件供应商部分公用的密钥，该密钥是在用户部分的保密算法中应用软件或软件供应商部分的标识符所生成的，第四密钥是用户部分公用的密钥，该密钥是在软件管理中心部分所拥有的软件或软件供应商部分的保密算法中应用用户部分的标识符所生成的。

# 说 明 书

## 软件保护系统

技术领域

本发明涉及一个软件保护系统。依据本发明的系统可用于保护诸如应用软件、操作系统等等，并可保护这些软件不受软件病毒的感染。

技术背景

未经授权非法拷贝应用程序、操作系统软件和实用程序是一个带有一定普遍性的问题。此前还没有发现一种好的方法来阻止这种非法拷贝行为，也没有一种令人满意的途径来保护软件免遭某些蓄意攻击和破坏软件的病毒的侵袭。因此，有必要寻找一种合适的保护软件的方法和途径。

发明内容

本发明的目的就是要实现一种软件保护系统。在该系统中，只有经过授权的用户才可以对软件进行操作，其他用户则不能使用该软件，并且能够检测到对该软件的非法改动同时发出警报。

依据本发明，可提供一种由以下三部分组成的保护软件的系统：软件供应商部分，随时准备为软件管理中心部分和用户部分提供程序；软件管理中心部分，与上述软件供应商部分相连，按预定的方式转换提供的程序并随时准备将此经过转换的程序提供给用户部分；用户部分，在使用程序期间，与上述软件供应商部分和软件管理中心部分相连，按预定的方式转换提供的程序，并将此经过转换的程序与上

述由软件管理中心所提供的经过转换的程序相比较，只有二者相同时才去执行该程序。

同时，依据本发明，还可提供一种由以下三部分组成的保护软件的系统：软件供应商部分，使用第一密钥对程序进行加密得到一经过加密的程序，再使用第二密钥对第一密钥进行加密得到经过加密的第一密钥，然后将此经过加密的程序提供给软件管理中心部分，并随时准备将此经过加密的程序和经过加密的第一密钥提供给用户部分；软件管理中心部分，与上述软件供应商部分相连，对提供的经过加密的程序进行转换得到一经过转换和加密的程序，然后使用第三密钥对该经过转换的程序进行加密得到一经过加密和转换的程序，再使用第四密钥对第三密钥进行加密得到经过加密的第三密钥，并随时准备将此经过加密和转换的程序及经过加密的第三密钥提供给用户部分；用户部分，在使用程序期间，与上述软件供应商部分和软件管理中心部分相连，按预定的方式对经过加密的程序进行转换得到经过转换的程序，然后使用第五密钥对经过加密的第三密钥进行解密得到解了密的第三密钥，再使用第三密钥对经过加密和转换的程序进行解密得到解了密的经过转换的程序，将此解了密的经过转换的程序与上述经过转换的程序相比较，只有当二者相同时才使用第六密钥解密第一密钥，然后使用该第一密钥去解密并执行该程序。

附图简介

图1是根据本发明某一实施例的软件保护系统所适用的一个信息处理网络图。

图2是根据本发明另一实施例的软件保护系统所适用的一个信息处理网络图。

实施本发明的最佳方式

依据本发明某一实施例的软件保护系统所适用的一个信息处理网络图如图1所示。该网络图中提供了一个软件车间1，即软件供应商部分，其中包括加密设备11和12。在软件车间1中，使用密钥K对程序P的全部或部分进行加密，得到经过加密的程序P1。其中，密钥K是特定于程序P的。经过加密的程序P1是不能执行的。经过加密的程序P1要向软件管理中心2进行注册。

根据来自用户部分3的请求，该用户已购买了经过加密的程序P1，使用用户的公开密钥P(u)对密钥K进行加密，得到经过加密的密钥K1，然后将此密钥K1发送到用户部分3。

软件管理中心部分2提供了转换设备21以及加密设备22和23。在软件管理中心部分2中，首先使用一种散列函数对由软件车间1注册的经过加密的程序P1进行压缩， 得到经过压缩和加密的程序P2，接着使用特定于程序P1的密钥r对该经过压缩和加密的程序P2进行加密，得到经过加密和压缩的程序P3，然后使用软件管理中心部分2的保密密钥S(sc)对密钥r进行加密，得到经过加密的密钥r1。因为经过加密的密钥r1以及经过加密和压缩的程序P3可以在不指定用户的情况下事先得到，所以它们可以和由软件车间1出售的经过加密的程序P1存放在同一存储介质中。

在用户部分3中，在购买程序时或购买程序之后，向软件车间1发出购买程序的通告和获取密钥的请求。由软件车间发来的经过加密的密钥K1作为安装软件的输入。在用户部分3中，通过使用加载软件和信息载体设备31来执行程序。设备31是连在程序执行设备32上的一个装置。程序执行设备32上可能连接的还有键盘显示设备、硬盘和磁盘一

类的存储器等等以及输入/输出设备。

在设备31中，有解密设备311、312、315和316，转换设备314，以及比较设备317。设备31里包含保密密钥、解密程序和用户的认证程序。设备31可以与用户将要用其执行程序的个人计算机上的打印口、RS232口等结合使用，以便进行诸如K1、P1、r1和P3一类数据的解密工作和程序的认证过程。设备31可以是，比方说，一片能与个人计算机相连的IC卡。

加密设备11、12、22和23可以由数据加密标准(DES)、快速数据加密算法(FEAL)(注册商标)等构成，但不必仅仅局限于这些例子。这些加密设备可以是同一类型的，也可以是不同类型的。解密设备311、312、315和316中的每一个都与其相应的加密设备成对出现。这些解密设备可以由数据加密标准(DES)的解密算法、快速数据加密算法(FEAL)等组成，但不必仅仅局限于这些例 子。

保密密钥S(u)和P(sc)是按将其写入设备31的存储器中的方式事先提供给用户部分的。使用散列函数的转换设备可以包含在设备31中，或者也可以将转换装置作为一个算法存储在程序执行设备32的存储介质中。可以将由软件供应商部分提供的经过加密的程序P1的部分或全部和经过加密的特定的密钥K1、连同由软件管理中 心部分提供的经过加密的密钥r和经过加密及压缩的程序P2存放在程序执行设备中的磁盘、随机访问存储器RAM、只读存储器ROM和光磁盘中，以便在程序执行设备中执行主处理过程。

使用加密信息的密钥的方法可以最好采用公开密钥系统和密钥预分配系统(KPS)。在公开密钥系统中，预先生成好公开密钥、与该公开密钥相关的公开文件以及保密密钥，公开密钥是单个分配的，保密密

钥是秘密管理的。公开密钥、与该公开密钥相关的公开文件以及保密密钥的生成和分配主要由软件管理中心部分的操作来完成。不过，也可以不受这种方式的限制而由用户部分、软件供应商部分或者二者合作来完成这一工作。生成每个公开密钥和保密密钥的具体内容的方法是对外公开的。

在密钥预分配系统(KPS)中，将另一方的标识符应用到自己一方特有的保密算法生成一个另一方常见的密钥。生成诸如保密算法之类的操作主要是在软件管理中心部分中进行的。软件管理中心部分各自拥有自己的中心算法。通过应用软件和软件供应商部分的标识符，即可生成特定的保密算法。

有关生成中心算法的方法、生成保密算法的方法、生成公共加密密钥的方法、以及机构和标识符的定义可在诸如日本待审专利公布第63-36634号和第63-107667号之类的文献中查到。

软件管理中心部分的操作可以在用户部分、软件供应商部分或二者合作完成。使用上述密钥的上述方法可优先选用，但是不必仅仅局限于此。对于加密算法，可采用诸如数据加密标准方法 (DES)、快速数据加密算法(FEAL)(注册商标)之类的算法。

图1所示网络图中所处理的软件可以是应用程序、操作系统程序、实用程序等等。图1所示网络图中的软件供应商部分(一个供给用户软件的机构)采用零售店的形式，如软件车间、有关的厂商、零售店、摊点、供给另一软件的软件或设备等等，有偿或无偿地为用户部分提供软件。软件供应商部分可以并入软件管理中心部分或用户部分。如果软件供应商部分处在使用一个软件的位置，那么软件供应商部分可以设定为用户部分。图1所示网络图中的用户部分以诸如用户自身、由用

户所拥有的软件来驱动其完成程序的执行的设备、连向那里的一台设备、软件自身等形式出现。

下面将讲述图1所示网络图中的操作。操作的前提条件是：(1)用户部分拥有包含其自身保密密钥的一台信息载体设备；(2)如果用户是未经授权的用户，目标程序将不工作；(3)可以自由地进行备份；(4)病毒问题的处理可以通过检查对数据的不正当修改来进行。

在操作中，首先，使用DES一类的加密算法用特定的密钥K对从软件供应商部分1发送到用户部分3的程序P的部分或全部进行加密，得到经过加密的程序P1。然后，向软件管理中心部分2注册该经过加密的程序P1。

在部分2中，使用某种散列函数对经过加密的程序P1进行压缩，得到经过压缩和加密的程序P2，该程序由某种加密算法，如DES，进行加密，得到经过加密和压缩 的程序P3。通过使用软件管理中心部分2的保密密钥S(sc)对密钥r进行加密。

在接收到P1、r1和P3时或之后，用户部分3向软件供应商部分1等通知这一接收事件。在软件供应商部分，通过使用用户部分的公开密钥P(u)对程序的特定密钥K进行加密，得到将发送到用户部分的经过加密的密钥K。在用户部分，通过使用专用的安装软件来完成K1、P1、r1和P3的安装。

在用户部分3，每次程序执行时，由加载软件通过使用信息载体设备31对P1进行解密，得到程序P1，通过使用散列函数对该经过解密的程序进行转换，得到经过压 缩的程序P2。通过使用软件管理中心部分2的公开密钥P(sc)对r1进行解密，得到r，然后使用该r对P3进行解密，得到经过解密的程序P2。将此经过解密的程序P2与上面提到的经

过压缩的程序P2进行比较以便能够检查程序P1是否经过了非正当的修改。如果检查到有非正当的修改，则可能发出警报。

因为经过加密的算法P1、经过加密的密钥r1以及经过加密和压缩的算法P3不与用户部分3的身份相关，所以它们可以预先生成好相同的，既可以从软件供应商部分1发来也可以从软件管理中心部分2发来。

与程序执行设备32相连的信息载体设备31最好是尺寸小、重量轻，具有占用空间不大的形状。另外，也可以不必提供信息载体设备，而由程序执行设备本身完成所有的操作。

依据本发明另一实施例的软件保护系统所适用的一个信息处理网络图如图2所示。该网络图中提供了一个软件车间1作为软件供应商部分，其中包括加密设备11和12以及密钥生成设备13。在软件车间1中，使用密钥K对程序P的全部或部分进行加密，得到经过加密的程序P1。其中，密钥K是特定于程序P的。经过加密的程序P1是不能执行的。经过加密的程序P1要向软件管理中心2进行注册。

根据来自用户部分3的请求，该用户已购买了经过加密的程序P1，通过使用用户部分的标识符A生成密钥预分配系统(KPS)的公共加密密钥K(SI · A)，用K(SI · A)对密钥K进行加密生成K1，然后将此经过加密的密钥K1发送到用户部分3。

软件管理中心部分2提供了转换设备21、加密设备22和23、以及密钥生成设备24。在部分2中，首先使用某种散列函数对由软件车间1注册的经过加密的程序P1进行压缩，得到经过压缩和加密的程序P2，接着使用特定于经过加密的程序P1的密钥r对P2进行加密，得到经过加密和压缩的程序P3，然后使用软件供应商部分或软件和用户部分公用的

加密密钥K(SI · A)对密钥r进行加密，得到经过加密的密钥r1。因为P3可以在不指定用户的情况下事先生成，所以P3可以和由软件车间1出售的经过加密的程序P1存放在同一存储介质中。在软件管理中心部分2，由软件供应商部分所拥有的保密算法既可以预先留存在那里，也可以后续再安装上。从这方面来讲，该特定的算法可以由软件管理中心部分所拥有。在这种情况下，当压缩后的软件等要发送到用户部分时，可以在软件管理中心部分的保密算法中使用用户部分的标识符来生成该密钥，而在用户部分的保密算法中使用软件管理中心部分的标识符来生成该密钥。

在用户部分3中，于使用程序时或购买程序之后，向软件供应商部分发出购买程序的通告，作为要求发送密钥的请求。在用户部分3中，将软件供应商部分1发来的经过加密的密钥K1输入到安装软件中，程序的执行是通过使用由安装软件所生成的 加载程序和与程序执行设备32相连的信息载体设备31来完成。信息载体设备31与程序执行设备32相连。程序执行设备32上连接的设备可能有键盘、显示设备、硬盘存储器、磁盘、输入/输出设备。在用户部分3中，软件供应商部分的标识符S(I)提供给密钥生成设备313。

在信息载体设备31中，包含保密密钥、解密程序和用户部分的认证程序。信息载 体设备31适合于与用户将要用其执行程序的个人计算机上的打印口、RS232C口等相连，以便进行K1、P1、r1和P3一类数据的解密工作和程序的认证过程。RS232C是由美国电子工业协会所发布的一个有关接口的标准。

图2的网络图中的加密设备11、12、22和23由数据加密标准方法(DES)的加密算法、快速数据加密算法(FEAL)(注册商标)等组成，但不

必仅仅局限于此。这些加密设备可以是同一类型的，也可以是不同类型的。解密设备311、312、315和316中的每一个都与其相应的加密设备成对出现。这些解密设备可以由数据加密标准(DES)的解密算法、快速数据加密算法(FEAL)等组成，但不必仅仅局限于这些例子。

保密算法预先提供给用户部分，并写入信息载体设备31的存储器中。用户部分所 拥有的由散列函数组成的转换设备可以预先包含在信息载体设备中，也可以作为算法存放在程序执行设备的存储器中。

可以将软件供应商部分1提供的经过加密的程序P1的部分或全部和经过加密的特定的密钥K1、连同软件管理中心部分2提供的经过加密的密钥$r_1$和经过加密及压缩的程序P3存放在程序执行设备中的磁盘、随机访问存储器RAM、只读存储器ROM和光磁盘中，并在程序执行设备中执行主处理过程。软件供应商部分的标识符A和用户部分所使用的软件可以与软件车间出售的经过加密的程序P1存放在同一存储介质中。

下面将讲述图2所示网络图中的操作。操作的前提条件是：(1)用户部分拥有包含其自身保密密钥的一台信息载体设备；(2)如果用户是未经授权的用户，目标程序将不工作；(3)可以自由地进行备份；(4)病毒问题的处理可以通过检查对数据的不正当修改来进行。

在操作中，首先，使用DES一类的加密算法用特定的密钥K预先对从软件供应商部分1发送到用户部分3的程序P的部分或全部进行加密，得到经过加密的程序P1。然后，向软件管理中心部分2注册该经过加密的程序P1。

在部分2中，使用某种散列函数对经过加密的程序P1进行压缩，得到经过压缩和加密的程序P2，该程序由某种加密算法，如DES，进行加密，得到经过加密和压缩的程序P3。密钥r由软件供应商部分或软件和

用户部分公用的加密密钥K(SI · A)进行加密，得到经过加密的密钥r1。

在接收到P1、r1和P3时或之后，用户部分3向软件供应商部分1等通知这一接收事件。

在软件供应商部分，通过使用软件供应商部分或软件和用户部分公用的加密密钥K(SI · A)对程序的特定密钥K进行加密，得到将发送到用户部分的经过加密的密钥K1。在用户部分，通过使用专用的安装软件来完成K1、P1、r1和P3的安装。

在用户部分3，每次程序执行时，由加载软件通过使用信息载体设备31对P1进行解密，得到程序P1，通过使用散列函数对该经过解密的程序进行转换，得到经过压缩的程序P2。通过使用软件供应商部分或软件和用户部分公用的密钥K(SI · A)对r1进行解密，得到r，然后使用r对P3进行解密，得到经过解密的程序P2。将此经过解密的程序P2与上面提到的经过压缩的程序P2进行比较以便能够判断程序P1是否经过了非正当的修改。如果检查到有某一非正当的修改，则可能发出警报。

因为经过加密的算法P1以及经过加密和压缩的算法P3不与用户部分3的身份相关，所以它们可以预先生成好相同的，既可以从软件供应商部分1发来也可以从软件管理中心部分2发来。

与程序执行设备32相连的信息载体设备31最好是尺寸小、重量轻，具有占用空间不大的形状。另外，也可以不必提供信息载体设备，而由程序执行设备本身完成所有的操作。

至此可以看出，在图1和图2所示的信息处理网络图中，只有经过授权的用户才可以对软件进行操作，其他用户则不能使用该软件，并且能够检测到病毒对该软件的非法改动同时发出警报。

图1

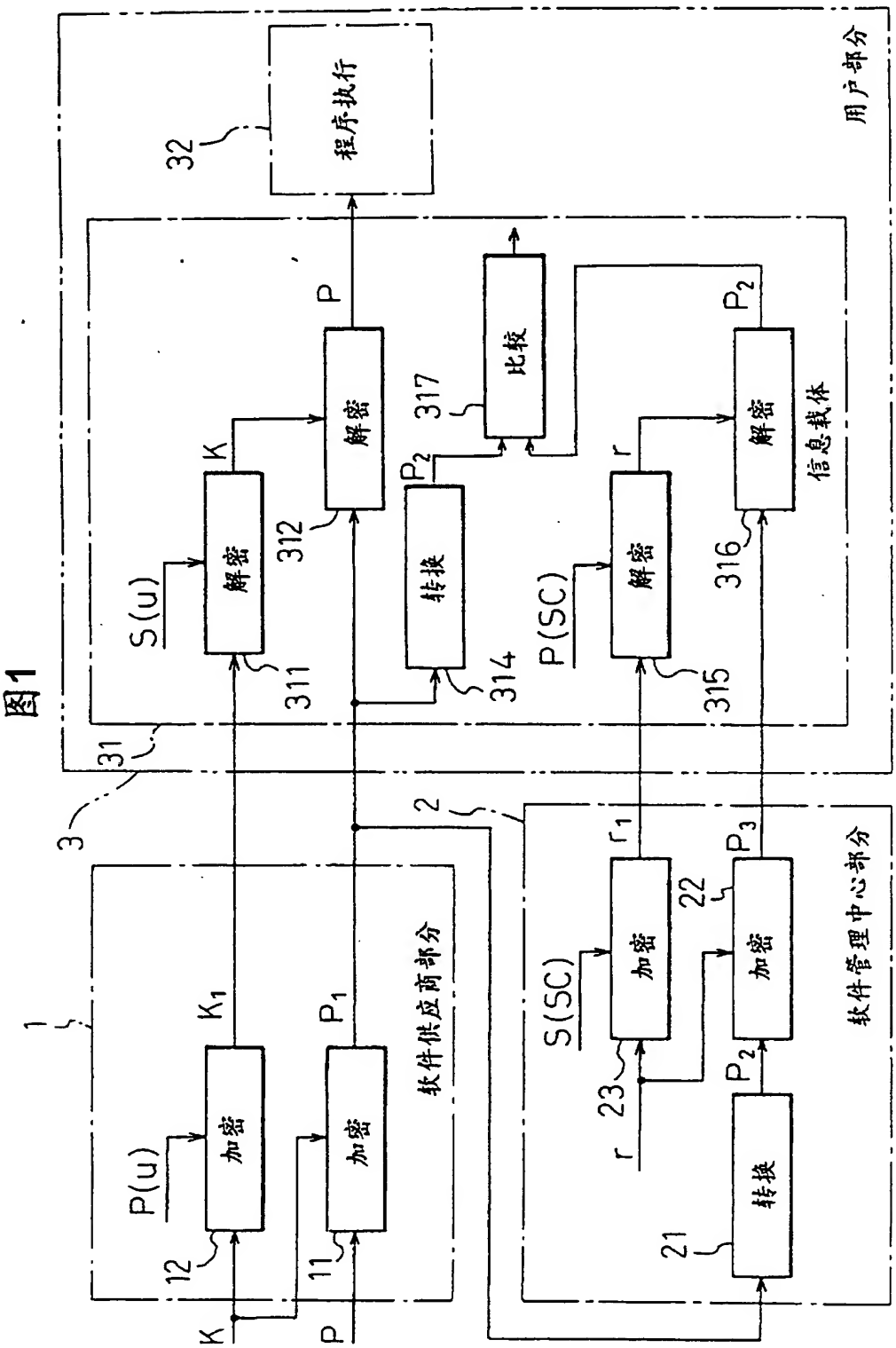
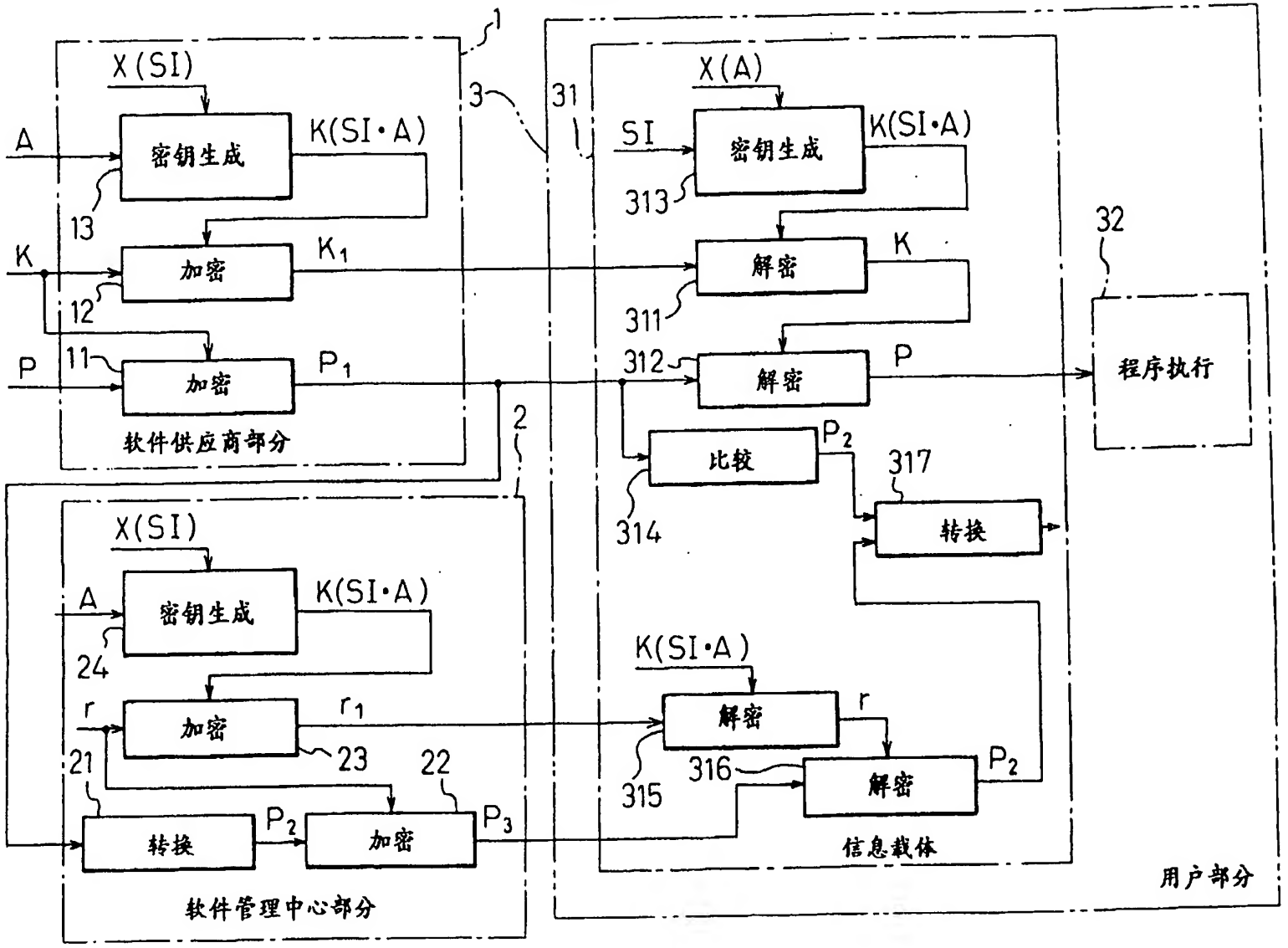

1
软件供应商部分
2
软件管理中心部分
3
用户部分
31
信息载体
32
程序执行
P(u)
加密
K1
12
K
P1
11
P
S(u)
解密
311
K
312
P
转换
314
P2
317
比较
P(SC)
解密
315
r
解密
316
P2
S(SC)
加密
r1
23
r
加密
22
P3
转换
21
P2

图2


1
3
X(SI)
A
密钥生成
K(SI·A)
13
K
加密
K1
12
P
11
加密
P1
软件供应商部分
2
X(SI)
A
密钥生成
K(SI·A)
24
r
加密
r1
23
21
22
转换
P2
加密
P3
软件管理中心部分
31
X(A)
SI
密钥生成
K(SI·A)
313
解密
K
311
312
解密
P
比较
P2
314
317
转换
K(SI·A)
解密
r
315
316
解密
P2
信息载体
32
程序执行
用户部分